UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF ILLINOIS EASTERN DIVISION

UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
)	42.05.074
v. ERIC ROGERS and ERIC CURTIS)	13 CR 952
)	
)	
Defendants.)	

MEMORANDUM OPINION

CHARLES P. KOCORAS, District Judge:

Defendants Eric Rogers ("Rogers") and Eric Curtis ("Curtis") (collectively "Defendants") seek to suppress electronic location evidence collected from Defendants' cell phones. For the reasons set forth below, Defendants' motion is denied.

BACKGROUND

For the purposes of providing context to the Defendants' motion to suppress we rely on the allegations contained in the criminal complaint and indictment filed against Defendants. The Defendants do not contest: (1) that the government had probable cause to believe that they were involved in numerous robberies committed with varying groups of individuals; and (2) the accuracy of the cell phone numbers used at the time of the robberies.

In early January 2013, the Federal Bureau of Investigation ("FBI") began investigating a series of armed robberies of cellular telephone stores in Illinois and Indiana. On February 5, 2013, three men were arrested after robbing an AT&T cellular store in LaPorte, Indiana ("LaPorte Robbery"). Those three men were identified as Daniel Wright ("Wright"), Marcus Harris and Individual A. One of the arrested individuals, Wright, agreed to speak with law enforcement officers and confessed to his involvement in the robberies. Wright admitted his involvement in the LaPorte robbery and also confessed to his involvement in multiple other cellular phone store robberies. Wright identified Rogers as the leader of the robbery crew. Wright went into detail about Rogers' role in recruiting participants, planning and executing the robberies. Wright provided Rogers' cellular phone number as 708-541-8767, and identified it as the number Rogers used to communicate with others during the robberies.

Based on this information, an application was submitted to a federal judge in the Northern District of Illinois on April 1, 2013, seeking cellular records from AT&T for the number provided by Wright. Law enforcement sought the disclosure of Rogers' cellular phone information under the Stored Communication Act ("SCA"), 18 U.S.C. § 2703(d) and confined the time period of their request from June 1, 2012 through March 29, 2013.

On April 8, 2013, the T-Mobile store in Deerfield, Illinois was robbed in a manner which matched the pattern of robberies of other cellular phone retail locations.

One of the captured robbers Andre Wadlington-Anthony ("Wadlington-Anthony") cooperated with law enforcement and admitted to his involvement as a member of the robbery crew. Wadlington-Anthony identified Curtis as an additional leader of the robbery operation. Wadlington-Anthony provided information concerning Curtis' scouting of perspective robbery locations, organizing the individuals to participate in the robberies and acting as the "look out" when the robbery was in progress. Wadlington-Anthony identified Curtis' mobile phone number as 708-969-6006.

Based on this additional information, an application was submitted to a federal judge in the Northern District of Illinois on April 11, 2013, seeking cellular phone records for Curtis' cellular phone from U.S. Cellular. Law enforcement sought the disclosure of Curtis' cellular phone information under 18 U.S.C. § 2703(d) for the time period of June 1, 2012 through April 10, 2013. On August 13, 2013, another individual that was suspected of participating in the robberies, Individual B, provided information to law enforcement about Rogers' and Curtis' shared participation in other robberies. This new information was the basis for another application which was submitted to a federal judge in the Northern District of Illinois, seeking cellular call records under 18 U.S.C. § 2703(d) for Rogers' and Curtis' cellular phones from AT&T and U.S. Cellular for the periods of March 29, 2013, through August 13, 2013.

On December 14, 2013, Defendants were arrested fleeing the scene of a T-Mobile cellular store robbery. On February 6, 2014, Defendants were indicted on charges of conspiracy to obstruct, delay and affect commerce in violation of Title 18

U.S.C. § 1951(a). On August 13, 2014, Defendants filed a joint motion to suppress the historic electronic location evidence gathered in the course of law enforcement's investigation.

LEGAL STANDARD

The Fourth Amendment provides that "[t]he right of people to be secure . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The amendment protects "people- and not simply 'areas' –against unreasonable searches and seizures." Katz v. United States, 389 U.S. 347, 353 (1967). "A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed," United States v. Jacobsen, 466 U.S. 109, 113 (1984), or when the government engages in an unlicensed physical intrusion of a constitutionally protected area in order to obtain information. Florida v. Jardines, 133 S.Ct. 1409, 1414–15 (2013). The party seeking suppression bears the burden of establishing that he had a reasonable expectation of privacy in what was searched. See United States v. Pitts, 322 F.3d 449, 456 (7th Cir. 2003); United States v. Meyer, 157 F.3d 1067, 1079 (7th Cir. 1998).

DISCUSSION

Defendants seek the suppression of all electronic location evidence gathered from third-party cellular companies in the course of the government's investigation. Defendants argue that suppression is warranted because: (1) the collection and acquisition of historic electronic location evidence data obtained under the SCA should only be acquired under the auspices of a search warrant; and (2) the SCA does not specifically authorize a warrantless search for location data.

Before addressing the merits of Defendants' motion to suppress, the Court will provide an abbreviated explanation of the technology at issue. Wireless technology operates through a network of cellular towers that emit radio frequencies capable of carrying the human voice and other data. Cellular phones are able to be located in one of two ways: by cell-site tracking, or by Global Positioning System ("GPS") signal tracking. Cell-site tracking relies on a cellular phones' requirement that they be constantly connected to a mobile network. To facilitate a cellular phone's connection to a mobile network, cellular phones are programmed to be constantly searching for the nearest cellular tower to ensure connection to the strongest signal. Once the phone selects the strongest signal, it transmits the user's identifying data so that the subscriber's network confirms the cell phones location to route any incoming calls. This constant search and submission of information occurs every few seconds. If the signal to a tower changes, or if a mobile phone moves, the mobile phone may switch its signal to a new tower. See Timothy Stapleton, Note, The Electronic

Communications Privacy Act and Cell Location Data, 73 Brook. L. Rev. 383, 387 (2007).

The recent introduction of "smart" phones equipped with GPS location has allowed mobile phones to be geographically located by utilizing the devices internal GPS system. In both "cell cite location" and "GPS location" situations, the government can either track a person in real time using live registration or GPS data, known as "prospective" records; or compile a list of a person's recent movements with their cell phone, known as "historic" records. *See* Stapleton, *supra*, at 388. With this in mind the Court turns to Defendants' motion to suppress.

1. No Legitimate Expectation of Privacy in Electronic Location Evidence

Defendants contend that the government obtaining historic electronic location evidence constitutes a search under the Fourth Amendment and therefore should require a warrant. In advocating for the suppression of historic electronic location evidence, Defendants principally rely on the United States Supreme Court's decision in *United States v. Jones*, 132 S. Ct. 945 (2012). In *Jones*, government agents surreptitiously attached a GPS monitoring device to the defendant's car for the purpose of monitoring his movements. Over the course of 28 days, agents were able to contemporaneously follow the defendant's movements in real time. The Supreme Court held that the government's actions constituted a warrantless search in violation of the Fourth Amendment because the government "physically occupied private property for the purpose of obtaining information." *Jones*, 132 S. Ct. at 949.

Defendants seek to draw a comparison between the GPS monitoring utilized in *Jones* and the electronic location evidence obtained in this case for the purposes of supporting suppression of the records.

At the outset it is important to note that the majority opinion in *Jones* utilized the "reasonable expectation of privacy" rubric from *Katz v. United States*, 389 U.S. 347 (1967) in conjunction with the trespassory nature of the GPS placement to render a decision. The *Jones* Court held that in addition to the *Katz* test, the Fourth Amendment also incorporated a common-law trespass test, so that a common law trespass into constitutionally protected areas could itself violate the Fourth Amendment. The Supreme Court expressly determined that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to [the] *Katz* analysis." *Jones*, 132 S. Ct. at 953. Absent a physical intrusion of Defendants' personal effects or property under the current circumstances, we will determine strictly whether Defendants had a reasonable expectation of privacy in their cellular phones historic electronic location records.

Initially, Defendants assert that the contemporaneous tracking of the GPS device utilized in *Jones* is the same as the electronic location evidence acquired from Defendants. The temporal distinction between *Jones* and the historical electronic location evidence obtained in this case is distinguishable. In *Jones*, the GPS monitoring enabled the government agents to monitor the whereabouts of Jones' vehicle in real time. Here, the historic electronic evidence provided only a historical

account of the Defendants' whereabouts in relation to the location of the cell towers utilized by the individual's cellular phones. A retroactive account of the Defendants' whereabouts would nullify the Supreme Court's concern over the "long-term monitoring of the movements" of an individual and renders a comparison inapplicable. *Jones*, 132 U.S. at 958. In the Defendants' Reply Brief, Defendants argue that the obtained electronic location evidence allowed the Government to contemporaneously track the Defendants' activities. However Defendants' factual assertion of "real time tracking" is not support by any evidence in the record. Absent any support in the record for Defendants' position, the Court finds that the collection of electronic evidence utilized in the case at bar is distinguishable from the tracking at issue in *Jones*.

Defendants further supports their position by pointing to the Eleventh Circuit's holding in *United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014), which deemed electronic location evidence as personal effects that an individual has a reasonable privacy interest in. However, it is important to note that the *Davis* decision has been withdrawn, and a rehearing *en banc* has been granted. *United States v. Davis*, 12 CR 12928, 2014 WL 4358411 (11th Cir. 2014). Thus the *Davis* opinion does not presently support or even offer persuasive authority for the Defendants' arguments.

Despite the historical nature of the electronic location evidence collected here, the way the records are created by third party telephone carriers in combination with their designed functionality does not elicit Fourth Amendment protection. Electronic

location records are created, maintained and produced by third party telephone carriers in the course of their normal business practices. See In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013). The Supreme Court has consistently held that there is no Fourth Amendment privacy right in third party business records that are conveyed to the government. Prior to the utilization of mobile phones, the Supreme Court held that a person has no legitimate expectation of privacy in a phone company's records of numbers dialed on a stationary telephone, and thus a defendant cannot invoke the Fourth Amendment when the police installed a pen register without a warrant. Smith v. Maryland, 442 U.S. 735, 745-46 (1979). As technology progressed and the emergence of cellular phones allowed third party cellular carriers to determine the location of phones in relation to their cell towers, court have followed Smith's line of reasoning. The Fifth Circuit recently concluded that Supreme Court precedent "does not recognize a situation where a conventional order for a third party's voluntarily created business records transforms into a Fourth Amendment search or seizure." The Fifth Court rejected the argument that using a court order, available through the SCA, to collect historical cell tower data without a showing of probable cause is unconstitutional. In re Application of U.S. for Historical Cell Site Data, 724 F.3d at 614-15; see also United States v. Guerro, 13-CR-50376, 2014 WL 4476565 (5th Cir. Sept. 11, 2014) (determining that *Riley v. California*, --U.S.--, 134 S. Ct. 2473 (2014) did not overturn In re Application of U.S. for Historical Cell Site Data). Although not explicitly addressing the issue of whether a

search warrant is required for cell site information, the Seventh Circuit acknowledged the total lack of any federal appellate decision accepting the premise that obtaining cell-site data from telephone carriers raises a Fourth Amendment concern. *See United States v. Thousand*, 558 Fed. Appx. 666, 670 (7th Cir. 2014); *see also United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012) (Holding that a criminal defendant does not have a reasonable expectation of privacy in cell phone location data as he traveled on public thoroughfares and therefore the collection of the data was not a search under the Fourth Amendment.).

Historic electronic location records fit squarely into the type of records the Supreme Court contemplated in *Smith*. Whether the numbers were dialed by the phone in the context of a pen register in *Smith* or, as here, signals emitted from a phone to allow for its functionality, these records are not an individual's private effects and belong to the third party cellular providers. Therefore, an individual user has no reasonable expectation of privacy in the historic electronic location evidence detailing the proximity of a cellular phone to the cellular tower. Without a reasonable expectation of privacy, it is unnecessary for the government to obtain a search warrant.

2. The SCA Authorizes a Recovery of Electronic Location Evidence

Defendants seem to contend the SCA does not authorize the disclosure of electronic location evidence. Intermixed throughout Defendants' argument on the limited scope of information permitted to be disclosed under § 2703(d), Defendants

Amendment. We have previously determined that Defendants do not have a reasonable expectation of privacy in historic electronic location evidence, and that a finding of probable cause for a search warrant is not necessary. Therefore, the Court will look to § 2703(c)(2) to determine if the SCA authorizes the collection of electronic location evidence.

Section 2703(c)(2) allows for the disclosure of "a record or other information pertaining to a subscriber to or a customer of" an electronic communications service. Specifically, § 2703(c)(2)(C) requires the disclosure of "local and long distance telephone connection records, or records of session times and duration. Since neither "record" nor "information" is defined within the SCA, the Court must look to the meaning of the terms in their ordinary usage. Black's Law Dictionary defines a "record" as an inclination to preserve or store. Black's Law Dictionary 1273 (6th ed. 1990). The term "information" in its relevant context means the conveyance of data. Cellular providers store data taken from cellular towers through which cellular phones calls are routed. Cellular phone companies utilize these records for the purposes of maintaining accurate billing of their customers' phone usage. See United States v. Madison, 11-CR-60285, 2012 WL 3095357 (S.D. Fla. July 30, 2012). The billing records contain the numbers called, the time the calls were made, and the cell towers used to begin and end the calls. Therefore, historic electronic location evidence is information which is permitted under §2703(c)(2) to be collected. In the case at bar,

Case: 1:13-cr-00952 Document #: 118 Filed: 10/09/14 Page 12 of 12 PageID #:281

the government sought and obtained a court order under 18 U.S.C. § 2703(d) to obtain

electronic location evidence from the Defendants' cellular phones. Section 2703(d)

allows for the disclosure of information set out in § 2703(c). 18 U.S.C. § 2703(d).

The Court concludes that the disclosure of electronic location evidence is authorized

under the SCA, and was properly disclosed here.

CONCLUSION

For the aforementioned reasons Defendants' motion to suppress is denied.

Charles P. Karnas

Charles P. Kocoras United States District Judge

Dated: 10/9/2014

- 12 -